数理解析研究所講究録
第1652巻 2009年 71-78

係数の小さい$\mathbb{K}[x]$上格子基底

大倉 安孝
OOKURA YASUTAKA *
筑波大学 数理物質科学研究科
GRADUATE SCHOOL OF PURE AND APPLIED SCIENCCES, UNIVERSITY OF TSUKUBA

Abstract

適切に定義されたノルムのもとで、ノルムの小さい格子基底を計算するアルゴリズムを考える。整数係数の一変数多項式環の格子基底が与えられたとき、我々は係数の小さい多項式で構成される新しい基底を計算する。数式処理において、多項式の係数をどのように扱うかは大きな問題である。例えば係数膨張がその良い例であり、本研究は多項式環上格子の係数について考察する初の研究である。我々は問題を整数格子の最近ベクトル問題に帰着させ、明解なアルゴリズムを構築する。

1 はじめに

格子基底縮小アルゴリズムは長い歴史をもっており、初めにLenstra、Lenstra、Lovászが整数環$\mathbb{Z}$上格子のアルゴリズムを開発した[7]。A. K. Lenstraはそのアルゴリズムを$\mathbb{F}_q[x]$上格子に拡張子した[8]。ここで、$\mathbb{F}_q$はq個の元からなる有限体である。von zur Gathenはの方法を非アルキメデス的付値環上の格子上に一般化し[11]、S. Paulusは関数体上の基底縮小アルゴリズムを開発した[10]。これらのアルゴリズムは多くの分野に応用がある。例えば、一変数多項式の因数分解[7]や多変数多項式の因数分解[8, 11]、Riemann-Roch空間の計算や[5]三次関数および楕円曲線の性質を計算することができる[3, 4]。

$\mathbb{Q}$を有理数体、$\mathbb{Q}[x]$を$\mathbb{Q}$上一変数多項式環、Lを$\mathbb{Q}[x]$上格子とする. Lの一組の基底Bが与えられたとき、格子の最短ベクトルとノルム最小の縮小基底を求めることができる[11]。ここで、ノルムは一般的にベクトルの要素である多項式の次数として定義される。そして、このような代数的な計算において頻繁に発生する係数膨張について、これまで十分な研究はなされてこなかった。係数膨張は$\mathbb{Z}[x]$上の格子でも問題となる。

我々はまず係数ベクトルのl_p-ノルムを定義し、$\mathbb{Z}[x]$-格子の短ベクトルを求める。短ベクトルの計算のためには以下の二つのアイディアを考える; (1) 係数ベクトルを使い、$\mathbb{Z}$-格子を構成する、(2)$\mathbb{Z}$-格子の最近ベクトル問題を解く。最近ベクトル問題 (closest vector problem, CVP) は整数論的アルゴリズムの問題で、格子に含まれない目標ベクトルが与えられたとき、それにもっとも近い格子ベクトルを探索することである。いくつかのアルゴリズムはCVPを厳密に解くが[6, 2]、その計算時間は$O(\exp(n))$である。ただし、nは格子の次元である。また、D. MicciancioはCVPがNP-困難であることを示した[9]。しかしL. Babaiによるアルゴリズム[1]は多項式時間で近似的にこの問題を解決する。話をもどすが、我々は$\mathbb{Z}[x]$-格子の短ベクトルを上の二つのアイディアを使うことで求めることができる。そして短ベクトルを使うことで、係数の小さい多項式からなる格子基底を再構成する。

今のところ[11]のように格子の最短ベクトルを求めることはできないうえ、我々のアプローチを$\mathbb{Q}[x]$上格子に適用することもできない。しかし多くの具体例から、この方法は有用であることが確認できている。また、本研究は多項式環上格子の係数を扱うことのできる初めての研究である。

*yasutaka@math.tsukuba.ac.jp

本論文の構成は以下の通りである。2章では必要な概念の定義をし、3章では短ベクトルの計算をする。4章では格子基底を再構成し、具体例を示す。

2 定義と準備

定義 2.1 ($\mathbb{Z}$-格子). 一次独立な n 個のベクトル $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n \in \mathbb{Z}^m$, $\boldsymbol{v}_i = (v_{i1}, \cdots, v_{im})(i = 1, \cdots, n$ かつ $n \leq m)$ をとる。基底 $B = \{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ により張られる格子を以下のように定義する。

$$\Lambda = \sum_{i=1}^{n} \mathbb{Z}\boldsymbol{v}_i.$$

定義 2.2 ($\mathbb{Z}[x]$-格子). 一次独立な n 個のベクトル $\boldsymbol{f}_1, \cdots, \boldsymbol{f}_n \in \mathbb{Z}[x]^m$, $\boldsymbol{f}_i = (f_{i1}, \cdots, f_{im})(i = 1, \cdots, n$ かつ $n \leq m)$ をとる。基底 $B = \{\boldsymbol{f}_1, \cdots, \boldsymbol{f}_n\}$ により張られる格子を以下のように定義する。

$$L = \sum_{i=1}^{n} \mathbb{Z}[x]\boldsymbol{f}_i.$$

定義 2.3 (l_p-ノルム). ベクトル $\boldsymbol{v} = (v_1, \cdots, v_n) \in \mathbb{Z}^n$ とする。$\boldsymbol{v}$ のノルムを以下のように定義する。

$$||\boldsymbol{v}||_p = (|v_1|^p + \cdots + |v_n|^p)^{1/p}, \quad p \in \mathbb{N}.$$

定義 2.4 (係数ノルム, l_p-ノルム). 多項式 $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ とする。多項式 f、ベクトル $\boldsymbol{f} = (f_1, \cdots, f_n) \in \mathbb{Z}[x]^n$、基底 $B = \{\boldsymbol{f}_1, \cdots, \boldsymbol{f}_n\} \subset \mathbb{Z}[x]^n$ のノルムをそれぞれ以下のように定義する。

- $|f|_p \stackrel{\text{def}}{=} (|a_n|^p + \cdots + |a_0|^p)^{1/p}, \quad p \in \mathbb{N},$
- $|\boldsymbol{f}|_p \stackrel{\text{def}}{=} (|f_1|^p + \cdots |f_n|^p)^{1/p},$
- $|B|_p \stackrel{\text{def}}{=} (|\boldsymbol{f}_1|^p + \cdots + |\boldsymbol{f}_n|^p)^{1/p}.$

以降簡単のために添字 p を書かず、単に $||\boldsymbol{v}||$, $|f|$, $|\boldsymbol{f}|$, $|B|$ と書く。

定義 2.5 ($\mathbb{Z}$-representation). ベクトル $\boldsymbol{f}_1, \cdots, \boldsymbol{f}_n \in \mathbb{Z}[x]^m$ に対し、
$d = \max\{\deg(f_{11}), \cdots, \deg(f_{1m}), \cdots, \deg(f_{n1}), \cdots, \deg(f_{nm})\}$ とする。係数 0 の項を適宜加えることによって、多項式 f_{ij} は

$$f_{ij} = a_{ij,d}x^d + a_{ij,d-1}x^{d-1} + \cdots + a_{ij,0},$$

と表現できる。ベクトル $\boldsymbol{f}_i$ の *$\mathbb{Z}$-representation* は以下のような係数リストのリストである。

$$\boldsymbol{v}_i = ((a_{i1,d}, \cdots, a_{i1,0}), \cdots, (a_{im,d}, \cdots, a_{im,0})).$$

ベクトル $\boldsymbol{v}_i$ は m 個のリストで構成されるが、単に $m(d+1)$ 次のベクトルとみなす。

例 2.1. $f_2 = (7x,\ 6x+1,\ 9x^2), f_3 = (5x^2+1,\ 3x,\ 7x^2+2) \in \mathbb{Z}[x]^3$ はそれぞれ
$v_2 = ((0,7,0),(0,6,1),(9,0,0)), v_3 = ((5,0,1),(0,3,0),(7,0,2))$ と表現される。

定義 2.6 ($\mathbb{Z}$-格子 $L_{\mathbb{Z}}$). 格子の基底を $B = \{f_1,\cdots,f_n\} \subset \mathbb{Z}[x]^m$ とする。ベクトル $f_1,\cdots,f_n$ と任意の自然数 γ に対して $\mathbb{Z}$-ベクトル $v_1, v_{20},\cdots,v_{2\gamma},\cdots,v_{n0},\cdots,v_{n\gamma}$, を考える。ここで、$v_1$ は f_1 の *$\mathbb{Z}$-representation*、v_{ji} は $x^i f_j$ $(0 \le i \le \gamma,\ 2 \le j \le n)$ の *$\mathbb{Z}$-representation* である。$\mathbb{Z}$-格子 $L_{\mathbb{Z}}$ は $v_{20},\cdots,v_{2\gamma},\cdots,v_{n0},\cdots,v_{n\gamma}$ で張られる格子とする。

注意 1. ここで

$$d = \max\{\deg(f_{11}),\cdots,\deg(f_{1m}),\deg(x^i f_{j1}),\cdots,\deg(x^i f_{jm})\} \quad (0 \le i \le \gamma,\ 2 \le j \le n),$$

とすると v_1 と v_{ji} は $k = m(d+1)$-次元ベクトルであり、$L_{\mathbb{Z}}$ の次元は k である。

3 アルゴリズムの概略

本論文において、ベクトルのノルムが比較的短かい場合そのベクトルを短ベクトルとよぶ。基底 $B = \{f_1,\cdots,f_n\} \subset \mathbb{Z}[x]^m$ が与えられたとき、以下の関係式を満たす短ベクトル g_1 を構成することを考える。

$$g_1 = f_1 + \sum_{i\neq 1}^{n} \mathbb{Z}[x] f_i. \tag{1}$$

我々のアルゴリズムは次の 4 ステップによって求める短ベクトル g_1 をみつける (詳細は次項)。

- 基底 $B = \{f_1,\cdots,f_n\}$ の入力。
- 定義 2.6 により $\mathbb{Z}$-ベクトル $v_1, v_{20},\cdots,v_{2\gamma},\cdots,v_{n0},\cdots,v_{n\gamma} \in \mathbb{Z}^k$, を計算し、格子 $L_{\mathbb{Z}}$ を構成する。(k は 注意 1 で言及した $L_{\mathbb{Z}}$ の次元).
- 最近ベクトル問題を解き、v_1 の最近ベクトル $v \in L_{\mathbb{Z}}$ を計算。
- ベクトル $v_g = v_1 - v \in \mathbb{Z}^k$ を計算し、v_g からベクトル g_1 を構成する。

3.1 $\mathbb{Z}$-格子 $L_{\mathbb{Z}}$ の構成

(1) で現れる表現には、$\mathbb{Z}$-representation による多項式ベクトルの加算が必要である。これは以下の様に簡単に実現できる。

命題 3.1 ($\mathbb{Z}$-representation による多項式の加算). ベクトル $f_2, f_3 \in \mathbb{Z}[x]^m$ の *$\mathbb{Z}$-representation* をそれぞれ $v_2 = (v_{21},\cdots,v_{2l}), v_3 = (v_{31},\cdots,v_{3l})$ とする。今、$f_2 + f_3$ の *$\mathbb{Z}$-representation* は

$$v_2 + v_3 = (v_{21} + v_{31},\cdots,v_{2l} + v_{3l}).$$

である。

証明. 定義 2.5 から明らか。 ■

例 3.1. 例 2.1 のベクトル $\boldsymbol{f}_2$ と $\boldsymbol{f}_3$ を考える。このとき、$\boldsymbol{f}_2+x\boldsymbol{f}_3 = (5x^3+8x,\ 3x^2+6x+1,\ 7x^3+9x^2+2x)$ である。これは $\mathbb{Z}$-representation によって以下のように表現できる。

$$\begin{array}{rl} & ((0,0,7,0),(0,0,6,1),(0,9,0,0)) \quad \leftarrow \boldsymbol{f}_2\text{の } \mathbb{Z}\text{-representation} \\ +) & ((5,0,1,0),(0,3,0,0),(7,0,2,0)) \quad \leftarrow x\boldsymbol{f}_3\text{の } \mathbb{Z}\text{-representation} \\ \hline & ((5,0,8,0),(0,3,6,1),(7,9,2,0)). \end{array}$$

(1) の右辺の表現について考える。直接 $\mathbb{Z}$-representation で表現することによって、以下の式を得る。

$$\boldsymbol{v}_g = \boldsymbol{v}_1 + \sum_{i=0}^{\infty}(\mathbb{Z}\boldsymbol{v}_{2i} + \cdots + \mathbb{Z}\boldsymbol{v}_{ni}). \tag{2}$$

ここで、$\boldsymbol{v}_g, \boldsymbol{v}_1, \boldsymbol{v}_{ji}$ はそれぞれ $\boldsymbol{g}_1, \boldsymbol{f}_1, x^i\boldsymbol{f}_j$ $(2 \le j \le n,\ i = 0, 1, 2, \cdots)$ の $\mathbb{Z}$-representation である。この表現では無限のベクトルを扱う必要がある。つまり $\mathbb{Z}$-representation の上限を定める必要があるが、現在 (1) を満たす最短ベクトル $\boldsymbol{g}_1$ を求めるための適切な上限の計算法は分かっていない。そこで上限 γ を適度に大きくとり、(2) の代わりに以下の表現を使う。

$$\boldsymbol{v}_g = \boldsymbol{v}_1 + \sum_{i=0}^{\gamma}(\mathbb{Z}\boldsymbol{v}_{2i} + \cdots + \mathbb{Z}\boldsymbol{v}_{ni}). \tag{3}$$

以降値 γ を shift-value という。ただし、$d = \max\{\deg(f_{11}), \cdots, \deg(f_{1m}), \cdots, \deg(f_{n1}), \cdots, \deg(f_{nm})\}$ に対して $\gamma < O(\exp(d))$ であることが望ましい。これより大きい γ はベクトル $\boldsymbol{g}_1$ を構成する多項式の次数を増大させ、次数を抑える研究結果である [11] に反するからである。また今、$\sum_{i=0}^{\gamma}(\mathbb{Z}\boldsymbol{v}_{2i} + \cdots + \mathbb{Z}\boldsymbol{v}_{ni})$ は格子 $L_{\mathbb{Z}}$ そのものである。

注意 2. 式 (3) は (1) で表現される全てのベクトルを含んでいないので、(3) は最短ベクトル $\boldsymbol{g}_1$ を含んでいるとは限らない。しかし多くの例において、小さな γ であっても短ベクトル $\boldsymbol{g}_1$ を得るのに十分であることが分かっている。

k を $L_{\mathbb{Z}}$ の次元とする。最近ベクトル問題を解くアルゴリズムによって、以下の関係式を満たす短ベクトル $\boldsymbol{v}_g$ を求めることを考える。

$$\boldsymbol{v}_g = \boldsymbol{v}_1 + \sum_{i=0}^{\gamma}(\mathbb{Z}\boldsymbol{v}_{2i} + \cdots + \mathbb{Z}\boldsymbol{v}_{ni}) \in \mathbb{Z}^k. \tag{4}$$

まず最近ベクトル問題の定義を述べる。

定義 3.2 (CVP). k 次元 $\mathbb{Z}$-格子 $L_{\mathbb{Z}}$ と目標ベクトル $\boldsymbol{t} \in \mathbb{Z}^k$ $(\boldsymbol{t} \notin L_{\mathbb{Z}})$ が与えられたとき、目標ベクトルに最も近い格子ベクトル $\boldsymbol{v}$ を求める。

以下の命題から、$\boldsymbol{v}_1$ を目標ベクトルに設定できることが分かる。

命題 3.3. $\boldsymbol{v}_1$ は $L_{\mathbb{Z}}$ に含まれない。

証明. $\boldsymbol{v}_1 \in L_{\mathbb{Z}}$ であると仮定すると

$$\boldsymbol{v}_1 = \sum_{i=0}^{\gamma}(z_{2i}\boldsymbol{v}_{2i} + \cdots + z_{ni}\boldsymbol{v}_{ni}), \quad z_{ji} \in \mathbb{Z}\ \ (2 \le j \le n).$$

と書ける。これは

$$\boldsymbol{f}_1 = \sum_{i=0}^{\gamma} z_{2i}x^i\boldsymbol{f}_2 + \cdots + \sum_{i=0}^{\gamma} z_{ni}x^i\boldsymbol{f}_n \in \mathbb{Z}[x]^m \tag{5}$$

と表現できることを意味するが、定義より $\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_n$ は $\mathbb{Z}[x]^m$ 上で互いに一次独立である。よって関係式 (5) は矛盾し、$\boldsymbol{v}_1 \notin L_{\mathbf{Z}}$ である。 ■

今、$\boldsymbol{v} \in L_{\mathbf{Z}}$ が $\boldsymbol{v}_1$ の最近ベクトルであるとし、

$$\boldsymbol{v}_g = \boldsymbol{v}_1 - \boldsymbol{v} \tag{6}$$

とおく。

命題 3.4. ベクトルを (6) のように計算すると、$\boldsymbol{v}_g$ は (4) を満たす最短ベクトルであり、$||\boldsymbol{v}_g|| \leq ||\boldsymbol{v}_1||$ が成り立つ。

証明. (4) において、ノルム $||\boldsymbol{v}_g||$ は目標ベクトル $\boldsymbol{v}_1$ と $L_{\mathbf{Z}}$ の任意の格子点との距離を表している。今 $\boldsymbol{v}$ は目標ベクトル $\boldsymbol{v}_1$ の最近格子点なので、その距離は最短である。よって $\boldsymbol{v}_g$ は最短ベクトルである。もし $||\boldsymbol{v}_g|| > ||\boldsymbol{v}_1||$ と仮定すると、$\mathbf{0}$ は $\boldsymbol{v}$ よりも $\boldsymbol{v}_1$ に近いことになり $\boldsymbol{v}$ が最近ベクトルであることに矛盾する。よって $||\boldsymbol{v}_g|| \leq ||\boldsymbol{v}_1||$ である。 ■

今、$\boldsymbol{v}_g$ が $\boldsymbol{g}_1$ の $\mathbb{Z}$-representation であるようにベクトル $\boldsymbol{g}_1 \in \mathbb{Z}[x]^m$ をとる。

例 3.2. ベクトル $\boldsymbol{v}_g = ((1,0,0),(2,0,0),(0,3,1))$ に対して $\boldsymbol{g}_1 = (x^2,\ 2x^2,\ 3x+1)$ である。

定理 3.5. $|\boldsymbol{g}_1| \leq |\boldsymbol{f}_1|$.

証明. 定義 2.3、2.4、2.5 より $|\boldsymbol{g}_1| = ||\boldsymbol{v}_g||$ かつ $|\boldsymbol{f}_1| = ||\boldsymbol{v}_1||$ である。また命題 3.4 より $||\boldsymbol{v}_g|| \leq ||\boldsymbol{v}_1||$ なので、$|\boldsymbol{g}_1| \leq |\boldsymbol{f}_1|$ となる。 ■

4 アルゴリズムの概要

まず短ベクトル $\boldsymbol{g}_1$ によっていかに $\mathbb{Z}[x]$-格子 L の基底を再構成するか述べる。

命題 4.1. 基底 $B_1 = \{\boldsymbol{g}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_n\}$ は L の基底である。

証明. $B = (\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_n), B_1 = (\boldsymbol{g}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_n) \in \mathbb{Z}[x]^{m \times n}$ とし、行列 $T \in \mathbb{Z}[x]^{n \times n}$ を B から B_1 への変換とする:

$$B_1 = BT.$$

今、

$$\boldsymbol{g}_1 = \boldsymbol{f}_1 + \sum_{i \neq 1}^{n} \mathbb{Z}[x]\boldsymbol{f}_i,$$

であるので、

$$T = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \mathbb{Z}[x] & 1 & & \\ \vdots & & \ddots & \mathbf{0} \\ \mathbb{Z}[x] & \mathbf{0} & & 1 \end{pmatrix}$$

と書ける。また $\det T = 1$ なので T はユニモジュラ行列である。格子の理論において、ユニモジュラ行列で変換される基底は同一の格子を張る。よって、B_1 は L の基底である。 ■

定理 4.2. $|B_1| \leq |B|$.

証明. 定義 2.4 と定理 3.5 より $|B|^p - |B_1|^p = |\boldsymbol{f}_1|^p - |\boldsymbol{g}_1|^p \geq 0$ である。 ■

4.1 再帰的ステップ

以下のように計算を繰り返す:

I. 基底 $B_1, B_2, \cdots, B_n$ を計算する ; i-ステップ $(i = 1, \cdots, n)$ では最近ベクトル問題を解いて

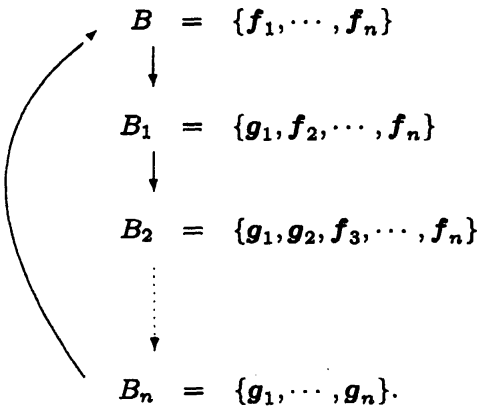
$$g_i = f_i + \sum_{j=1}^{i-1} \mathbb{Z}[x] g_j + \sum_{j=i+1}^{n} \mathbb{Z}[x] f_j$$

を満す短ベクトルを計算し、基底

$$B_i = \{g_1, \cdots, g_i, f_{i+1}, \cdots, f_n\}$$

をとる。

II. $|B_n| < |B|$ であれば $B \leftarrow B_n$ とし同様の計算をくりかえす。



命題 4.3. 上述のアルゴリズムは正常に終了する。

証明. 命題 4.1 と同様に $B_{i-1} = (g_1, \cdots, g_{i-1}, f_i, \cdots, f_n)$, $B_i = (g_1, \cdots, g_i, f_{i+1}, \cdots, f_n) \in \mathbb{Z}[x]^{m \times n}$ とする。また $B_i = B_{i-1} T_i$ $(1 \leq i \leq n)$ を満す行列 $T_i \in \mathbb{Z}[x]^{n \times n}$ を考える。明かに $\det(T_i) = 1$ かつ $|B_i| \leq |B_{i-1}|$ である。よって、B_i は同一の格子の基底である。また、次の条件のどちらかを満している; (1)$|B_n| = |B|$ もしくは (2)$|B_n| < |B|$。もし (1) が満されていれば、アルゴリズムは終了する。ノルムは整数であり下界があるので、(2) は有限回しか現れない。 ■

5 Example

l_2-ノルムで、以下の基底を使う。

基底 B	$\{f_1, f_2, f_3\} \in \mathbb{Z}[x]^3$ $f_1 = (4x^2,\ 5x + 2,\ 10x^2 + 3)$ $f_2 = (7x,\ 6x + 1,\ 9x^2)$ $f_3 = (5x^2 + 1,\ 3x,\ 7x^2 + 2)$
ノルム	$\lvert B\rvert = \sqrt{409}$
shift-value	3

$f_1, f_2, xf_2, x^2f_2, x^3f_2, f_3, xf_3, x^2f_3, x^3f_3$ の $\mathbb{Z}$-representation は

$$
\begin{aligned}
v_1 &= (0,0,0,4,0,0,0,0,0,5,2,0,0,0,10,0,3).\\
v_{20} &= (0,0,0,0,7,0,0,0,0,6,1,0,0,0,9,0,0),\\
v_{21} &= (0,0,0,7,0,0,0,0,6,1,0,0,0,9,0,0,0),\\
v_{22} &= (0,0,7,0,0,0,0,6,1,0,0,0,9,0,0,0,0),\\
v_{23} &= (0,7,0,0,0,0,6,1,0,0,0,9,0,0,0,0,0),\\
v_{30} &= (0,0,0,5,0,1,0,0,0,3,0,0,0,0,7,0,2),\\
v_{31} &= (0,0,5,0,1,0,0,0,3,0,0,0,0,7,0,2,0),\\
v_{32} &= (0,5,0,1,0,0,0,3,0,0,0,0,7,0,2,0,0),\\
v_{33} &= (5,0,1,0,0,0,3,0,0,0,0,7,0,2,0,0,0),
\end{aligned}
$$

である。ベクトル v_{2i}, v_{3i} $(0 \leq i \leq 3)$ は格子 $L_{\mathbb{Z}}$ を張り、目標ベクトル v_1 の最近ベクトル $v \in L_{\mathbb{Z}}$ は

$$v = v_{30}$$

である。よって、

$$
\begin{aligned}
v_g &= v_1 - v\\
&= (0,0,0,-1,0,-1,0,0,0,2,2,0,0,0,3,0,1).
\end{aligned}
$$

とする。以上より

$$g_1 = (-x^2-1, 2x+2, 3x^2+1) \quad (= f_1 - f_3)$$

を得る。この計算を繰り返し、以下の基底 B' を得る。

基底 B'	$\{g_1, g_2, g_3\}$ $g_1 = (-x^2-1, 2x+2, 3x^2+1)$ $g_2 = (-4x^2+7, x-1, -x^2-3)$ $g_3 = (4x^4+3, -x^3+x^2-x-4, x^4+4x^2)$
ノルム	$\|B'\| = \sqrt{158}$

6 今後の課題

現在のところ本研究の結果は非常に弱い; 新しい基底が与えられた基底より大きくはない、ということがいえるだけである。もし与えられた基底が大きければ最近ベクトル問題により、我々のアルゴリズムはたしかに小さな基底を計算することができる。しかし基底やベクトルのノルムを厳密に評価し、格子の最短ベクトルを見つけられるのか考察する必要がある。また、縮小基底の適切な定義も重要である。

7 謝辞

有用な助言をして下さった佐々木建昭先生、および議論をしてくれた友人に感謝します。

参 考 文 献

[1] Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica **6**(1), 1-13 (1986).

[2] Banihashemi, A. H., Khandani, A. K.: On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis. IEEE Trans. Inform. Theory **44**(1), 162-171 (1998).

[3] Bauer, M. L.: The arithmetic of certain cubic function fields. Math. Comp. **73**(245), 387-413 (2004).

[4] Galbraith, S. D., Paulus, S. M., Smart, N. P.: Arithmetic on superelliptic curves. Math. Comp. **71**(237), 393-405 (2002).

[5] Hess, F.: Computing Riemann-Roch spaces in algebraic function fields and related topics. J. Symbolic Comput. **33**(4), 425-445 (2002).

[6] Kannan, R.: Minkowski's convex body theorem and integer programming. Math. Oper. Res. **12**(3), 415-440 (1987).

[7] Lenstra, A. K., Lenstra, H. W. Jr., Lovász, L.: Factoring Polynomials with Rational Coefficients. Math. Ann. **261**(4), 515-524 (1982).

[8] Lenstra, A. K.: Factoring Multivariate Polynomials over Finite Fields. J. Comput. System Sci. **30**(2), 235-248 (1985).

[9] Micciancio, Daniele: The hardness of the closest vector problem with preprocessing. IEEE Trans. Inform. Theory **47**(3), 1212-1215 (2001).

[10] Paulus, S.: Lattice basis reduction in function fields. Lecture Notes in Comput. Sci. **1423**, Springer, Berlin, (1998).

[11] von zur Gathen, J.: Hensel and Newton Methods in Valuation Rings. Math. Comp. **42**(166), 637-661 (1984).